LARSON ▸ NEWMAN

Intellectual Property Law

5914 West Courtyard Drive, Suite 200
Austin, TX • 78730
Phone: 512-439-7100
Fax: 512-439-7199

FACSIMILE COVER SHEET

DATE: July 24, 2006

TO: Examiner Shin Hon CHEN FAX NO.: 571-273-8300
USPTO GPAU 2131

FROM: Ryan S. Davidson
Reg. No. 51,596

RE: BRIEF IN SUPPORT OF APPEAL

U.S. APP NO.:	09/995,308
FILING DATE:	November 27, 2001
APPLICANT(S):	Paul DUCHARME
ATTY DKT NO.:	VIXS.0100300 (1459-0100300)
TITLE:	A MONOLITHIC SEMICONDUCTOR DEVICE FOR PREVENTING EXTERNAL ACCESS TO AN ENCRYPTION KEY

NO. OF PAGES (INCL. COVER SHEET): **29**

Attached please find:

☒ Transmittal Form (1 pg)

☒ Fee Transmittal Form (1 pg) (in duplicate)

☒ Brief in Support of Appeal (25 pgs)

RECEIVED
CENTRAL FAX CENTER
JUL 24 2006

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 28

Application Number	09/995,308
Filing Date	November 27, 2001
First Named Inventor	Paul DUCHARME
Art Unit	2131
Examiner Name	Shin Hon CHEN
Attorney Docket Number	VIXS.0100300 (1459-0100300)

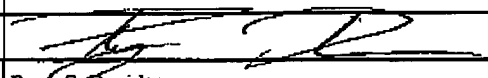
ENCLOSURES *(Check all that apply)*

- [✔] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [✔] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please identify below):

Remarks

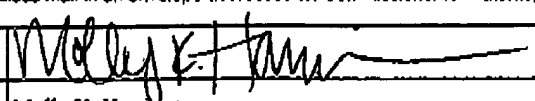
CUSTOMER NO.: 29331

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	LARSON NEWMAN ABEL POLANSKY & WHITE, LLP		
Signature			
Printed name	Ryan S. Davidson		
Date	July 24, 2006	Reg. No.	51,596

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Molly K. Harrison	Date	July 24, 2006

RECEIVED
CENTRAL FAX CENTER
JUL 24 2006

PTO/SB/17 (12-04v2)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2005

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 250.00

Complete if Known	
Application Number	09/995,308
Filing Date	November 27, 2001
First Named Inventor	Paul DUCHARME
Examiner Name	Shin Hon CHEN
Art Unit	2131
Attorney Docket No.	VIXS.0100300 (1459-0100300)

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1835 Deposit Account Name: ViXS Systems, Inc.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☑ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 20 or HP =	_____	x _____	= _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 3 or HP =	_____	x _____	= _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($)	Fee Paid ($)
_____	_____

3. APPLICATION SIZE FEE

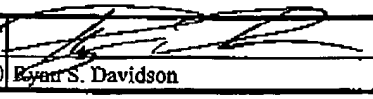
If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(c)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
_____ - 100 =	_____ / 50 =	_____ (round up to a whole number)	x _____	= _____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Appeal Brief	250.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 51,596	Telephone 512-439-7100
Name (Print/Type)	Ryan S. Davidson		Date July 24, 2006

RECEIVED
CENTRAL FAX CENTER

JUL 24 2006

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	Paul DUCHARME		
Title:	A MONOLITHIC SEMICONDUCTOR DEVICE FOR PREVENTING EXTERNAL ACCESS TO AN ENCRYPTION KEY		
App. No.:	09/995,308	Filed:	11/27/2001
Examiner:	CHEN, Shin Hon	Group Art Unit:	2131
Customer No.:	29331	Confirmation No.:	9477
Atty. Dkt. No.:	VIXS.0100300 (1459-0100300)		

Mail Stop Appeal Brief - Patents
The Board of Patent Appeal and Interferences
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

BRIEF IN SUPPORT OF APPEAL

Ryan S. Davidson, Reg. No. 51,596
LARSON NEWMAN ABEL POLANSKY & WHITE LLP
(512) 439-7100 (phone)
(512) 439-7199 (fax)

07/26/2006 AWONDAF1 00000008 501835 09995308
01 FC:2402 250.00 DA

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(1)):

TABLE OF CONTENTS

The final page of this brief before the beginning of the Appendix of Claims bears the agent's signature.

I. REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is ViXS Systems, Inc., the assignee in the entirety, as evidenced by the assignment recorded at Reel 012329, Frame 0143.

II. RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c)(1)(ii))

There are no interferences or other appeals that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS (37 C.F.R. § 41.37(c)(1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

There are eighteen (18) claims pending in the application.

B. STATUS OF ALL THE CLAIMS

1. Claims pending:

   Claims 1, 17-22, 24-33, and 41.

2. Claims withdrawn from consideration but not canceled:

   NONE.

3. Claims allowed:

   NONE.

4. Claims objected to:

   NONE.

5. Claims rejected:

   Claims 1, 17-22, 24-33, and 41 are rejected under 35 U.S.C. § 103(a).

6. Claims canceled:

Claims 2-16, 23, and 34-40.

C. CLAIMS ON APPEAL

There are five (5) claims on appeal, claims 1, 17, 31, 33 and 41.

IV. STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

No amendments have been submitted subsequent to the final Office Action mailed January 24, 2006 (hereinafter, "the Final Rejection") or the Advisory Action mailed April 14, 2006 (hereinafter, "the Advisory Action").

V. SUMMARY OF THE CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

The following summary is provided to give the Board the ability to quickly determine where the claimed subject matter appealed herein is described in the present application and is not to limit the scope of the claimed invention.

Independent claim 1 recites the features of a monolithic semiconductor device (e.g., monolithic semiconductor device 200, FIG. 2) comprising a memory location (e.g., key register 130, FIG. 2) having an output port, wherein a data value to be stored in said memory location is observable only internally to the monolithic semiconductor device (see, e.g., p. 6, lines 6-13). Claim 1 further recites the features of the monolithic semiconductor device comprising an asymmetrical encryption engine (e.g., encryption engine 120, FIG. 2) having an input port coupled to the output port of the memory location and an output port to provide a symmetrical encryption key based on the data value (see, e.g., p. 5, lines 7-19) and a symmetrical encryption engine (e.g., additional component 150, FIG. 2) having an input port coupled to an output port of

the asymmetrical encryption engine, wherein the symmetrical encryption engine is to perform an encryption function using the symmetrical encryption key (see, e.g., p. 5, lines 16-19). Claim 1 further recites the features of wherein the monolithic semiconductor device further includes at least one silicon die pad (e.g., input/output die pads 235-237, FIG. 2) having an input coupled to the output port of said memory location to provide temporary access to said memory location (see, e.g., p. 9, line 24 – p. 10, lines 2).

Independent claim 17 recites the features of a monolithic semiconductor device (e.g., monolithic semiconductor device 300, FIG. 3) comprising an external data port (e.g., external port 110, FIG. 3) having an input and an output, a first encryption engine (e.g., encryption engine 120, FIG. 3) having an input coupled to the input of said external data port and an output, and a second encryption engine (e.g., additional component 150, FIG. 3) having an input coupled to the output of the first encryption engine and an output. Claim 17 further recites the features of wherein the monolithic semiconductor device further comprises a memory location (e.g., key register 130, FIG. 3) having an output coupled to the input of said first encryption engine, an isolation portion (e.g., isolation portion 310, FIG. 3) coupled to the output of said memory location and to the input of said external data port, wherein said isolation portion is modifiable to permanently prevent access of said memory location by the external data port (see, e.g., FIGS. 4 and 5, p. 10, lines 17-29), and wherein the first encryption engine is to provide a first encryption key based on a value stored at said memory location to said second encryption engine (see, e.g., p. 11, lines 1-18).

Dependent claim 31, which depends from claim 17, recites the additional features of at least one silicon die pad (e.g., input/output die pads 235-237, FIG. 2) coupled to the output of

said memory location to provide temporary external access to said memory location (see, e.g., p. 9, line 24 – p. 10, lines 2).

Independent claim 33 recites the features of accessing, by a first encryption engine (e.g., encryption engine 120, FIG. 7) internal to a monolithic semiconductor device (e.g., monolithic semiconductor device 700, FIG. 7), data from a memory location (e.g., key register 130, FIG. 7) internal to the monolithic semiconductor device, wherein the memory location is accessible only internal to the monolithic semiconductor device (see, e.g., p. 6, lines 6-13), and generating, at the first encryption engine, a first encryption key based on the data from the memory location, wherein the data represents a second encryption key (see, e.g., see, e.g., p. 11, lines 1-18 and FIG. 6). Claim 33 further recites the features of providing the first encryption key for storage in the memory location (see, e.g., p. 11, lines 1-18) and providing the first encryption key to a second encryption engine (e.g., descrambler 150, FIG. 7) internal to the monolithic semiconductor device (see, e.g., p. 12, lines 21-25). Claim 33 further recites the features of performing an encryption function at the second encryption engine using the first encryption key (see, e.g., p. 13, lines 5-8).

Independent claim 41 recites the features of a monolithic semiconductor device (e.g., monolithic semiconductor device 200, FIG. 2) comprising an encryption engine (e.g., encryption engine 120, FIG. 2) having an input, a memory location (e.g., key register 130, FIG. 2) having an output coupled to the input of the first encryption engine, wherein a data value to be stored in said memory location is observable only internally to the monolithic semiconductor device (see, e.g., p. 6, lines 6-13), and at least one silicon die pad (e.g., input/output die pads 235-237, FIG. 2) having an input coupled to the output port of said memory location to provide temporary access to said memory location (see, e.g., p. 9, line 24 – p. 10, lines 2).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

A. Claim 1, 33, and 41 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,563,950 to Easter *et al.* (hereinafter, "Easter") in view of U.S. Patent No. 5,850,443 to Van Oorschot *et al.* (hereinafter, "Van Oorschot) as set forth in the Advisory Action.

B. Claims 17 and 31 are rejected under 35 U.S.C. § 103(a) as unpatentable over Easter in view of Van Oorschot and further in view of U.S. Patent Pub. No. 2002/0145931 to Pitts (hereinafter, "Pitts") as set forth in the Advisory Action.

VII. ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

Based on the arguments and issues below, none of the claims stand or fall together, because in addition to having different scopes, each of the independent claims has a unique set of issues relating to its rejection and appeal as indicated in the arguments below:

A. Rejection of Claims 1, 33, and 41 under 35 U.S.C. § 103(a)

In Section 3 of the Advisory Action, claims 1, 33, and 41 are rejected under 35 U.S.C. § 103(a) as unpatentable over a combination of Girod and Van Oorschot.

As stated in MPEP § 2143, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the

reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Also, as stated in MPEP § 2143.01, obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Further, as stated in MPEP § 2143.01, to establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). That is, "[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 165 USPQ 494, 496 (CCPA 1970). Additionally, as stated in MPEP § 2141.02, a prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. W.L. Gore & Associates, Inc. v. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), cert. denied, 469 U.S. 851 (1984). Finally, if an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

1. Rejection of Claims 1 and 41

For ease of reference, claims 1 and 41 are reproduced in its entirety below:

1. (Previously Presented) A monolithic semiconductor device comprising:
a memory location having an output port, wherein a data value to be stored in said memory location is observable only internally to the monolithic semiconductor device;
an asymmetrical encryption engine having an input port coupled to the output port of the memory location and an output port to provide a symmetrical encryption key based on the data value;
a symmetrical encryption engine having an input port coupled to an output port of the asymmetrical encryption engine, wherein the symmetrical encryption engine is to perform an encryption function using the symmetrical encryption key; and
at least one silicon die pad having an input coupled to the output port of said memory location to provide temporary access to said memory location.

41. (Previously Presented) A monolithic semiconductor device comprising:
an encryption engine having an input;
a memory location having an output coupled to the input of the first encryption engine, wherein a data value to be stored in said memory location is observable only internally to the monolithic semiconductor device;
at least one silicon die pad having an input coupled to the output of said memory location to provide temporary access to said memory location.

a) Easter fails to disclose or suggest a silicon die pad having an input coupled to the output port of a memory location to provide temporary access as recited by claims 1 and 41

Claim 1 recites the features of a memory location having an output port, wherein a data value to be stored in said memory location is observable only internally to the monolithic semiconductor device, and **at least one silicon die pad having an input coupled to the output port of said memory location to provide temporary access to said memory location.** Claim 41 also recites these features. The Office asserts the key array 25/fuse array 51 of Easter discloses the claimed memory location feature and that Figure 2 of Easter and the passage of Easter at column 4, lines 50-65 disclose the claimed silicon die pad feature. Advisory Action, pp. 2-3.

The Office further clarifies its position by stating that

> Easter discloses than an IC chip that includes memory locations (fuse array/key array) and the public key engine is used to generate the key required by DES engine and the key is stored in key array (FIG. 5, column 8 lines 18-26). Furthermore, the key array is the temporary storage area that takes output of the RSA engine and the integrated circuits are well known to contain die pads.

Advisory Action, p. 9.

For ease of reference, the cited passages of Easter at column 4, lines 50-65 and col. 8, lines 18-26 are reproduced below:

> Single IC chip 63 includes input buffer 15 and output buffer 17 that control I/O with CPU 13 over internal busses 35 and I/O bus 14. An RSA engine 57 is provided as a public key cryptography engine. All of these elements are interconnected by bussing 35. Further, key storage is provided by a combination of a fuse array 51 and a key array 25 that are connected to RSA engine 57 via key transfer busses 37.
>
> Key storage facilities for RSA engine 57 are provided by a combination of key array 25 and fuse array 51. To recall, public key cryptographic engines (such as RSA engine 57) require the use of a private key and a public key. In accordance with the present invention, the private key is contained within a non-volatile memory comprising fuse array 51, while the public key is loadable into a volatile memory (such as a random access memory, a "RAM") comprising key array 25.

Easter, col. 4, lines 50-65.

> Keys for DES encryption engine 21 are stored in key array 25. This is a programmable storage area comprising, for example, RAM. Operationally, keys are transferred for use as DES master keys via public key cryptography techniques using RSA engine 57. One technique for such transfer is described in Munck et al., incorporated by reference hereinabove. Advantageously, using the techniques of the present invention, the private key is secured and the disadvantages of prior manual key loading systems are overcome.

Id., col. 8, lines 18-26.

Contrary to the assertions of the Office, Easter fails to disclose or suggest a silicon die pad having an input coupled to the output port of a memory location in any manner, much less a silicon die having an input coupled to the output port of a memory to provide temporary access to the memory location as recited by claims 1 and 41. As noted above, the Office asserts "the

integrated circuits are well known in the art to contain die pads." Advisory Action, p. 9. While the Applicant does not disagree with the proposition that integrated circuits are well known to contain die pads, the Office errs in the unreasonable extension of this general statement to conclude that it is well known to use silicon die pads that have an input connected to an output port of a memory location to provide temporary access to the memory location. To wit, the Office has failed to provide any reference that demonstrates that it is well known to connect the input of a silicon die pad to the output port of a memory location that is used to store a data value that is observable only internally to a monolithic semiconductor device, much that a silicon die pad connected in such a manner is to provide temporary access to such a memory location. Further, it is submitted that it is not in fact well known to use a silicon die pad in the manner provided by claims 1 and 41.

Turning to the above-reproduced passages of Easter cited by the Office in support of its assertion that Easter discloses or suggests a silicon die pad connected to the output port of a memory location, neither of these passages discloses or suggests that an output of the key array 25/fuse array 51 (which the Advisory Action asserts is equivalent to the claimed memory location) is connected to a silicon die pad, much less that they are connected to a silicon die pad for temporary access. Rather, these passages, as well as FIG. 5 of Easter, merely describe the storage of keys in the key array 25/fuse array 51. Moreover, it is noted that Easter fails to disclose die pads in any capacity.

In view of the foregoing, it is respectfully submitted that Easter fails to disclose, or even suggest, at least one silicon die pad having an input coupled to the output port of a memory location to provide temporary access to said memory location. The Office therefore errs in its assertion that Easter discloses or suggests this recited feature of claims 1 and 41.

b) The proposed combination of Easter and Van Oorschot fails to disclose or suggest a silicon die pad having an input coupled to the output port of a memory location to provide temporary access as recited by claims 1 and 41

As discussed in section (a) above, Easter fails to disclose or suggest at least the feature of at least one silicon die pad having an input coupled to the output port of a memory location to provide temporary access to said memory location as recited by claims 1 and 41. The Office does not assert that Van Oorschot discloses or suggests this claimed feature, nor in fact is this feature disclosed or suggested by Van Oorschot. Accordingly, Easter and Van Oorschot, individually or in combination, fail to disclose or suggest each and every feature recited by claims 1 and 41.

c) Claims 1 and 41 are allowable under 35 U.S.C. § 103(a)

As discussed in sections (a) and (b) above, the proposed combination of Easter and Van Oorschot fails to disclose or suggest each and every feature recited by claims 1 and 41. Accordingly, the Office fails to establish a *prima facie* case of obviousness in support of its rejection of claims 1 and 41. Claims 1 and 41 therefore are allowable under 35 U.S.C. § 103(a).

2. Rejection of Claim 33

For ease of reference, claim 33 is reproduced in its entirety below:

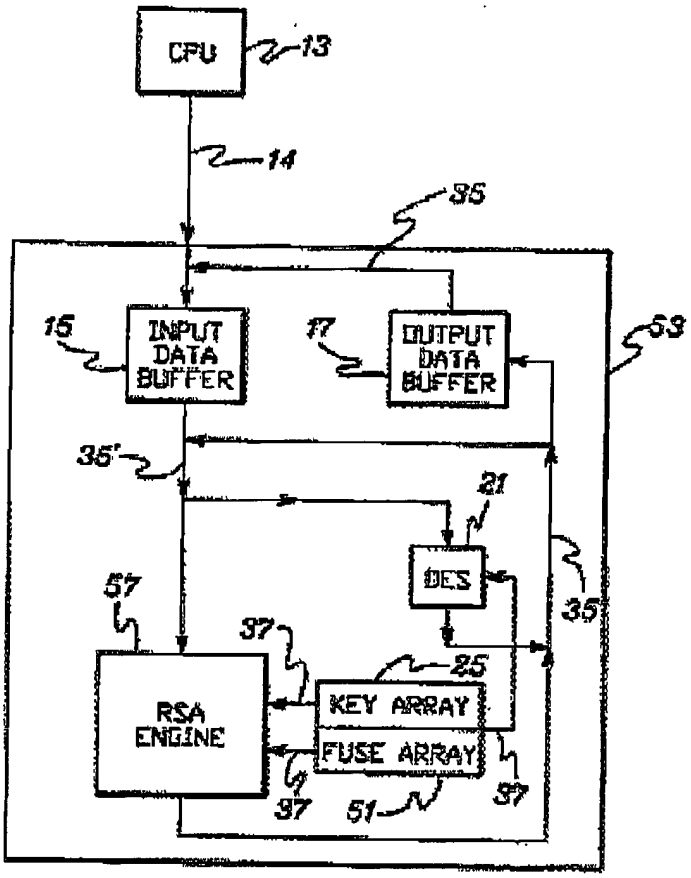
33. (Previously Presented) A method comprising:
accessing, by a first encryption engine internal to a monolithic semiconductor device, data from a memory location internal to the monolithic semiconductor device, wherein the memory location is accessible only internal to the monolithic semiconductor device;
generating, at the first encryption engine, a first encryption key based on the data from the memory location, wherein the data represents a second encryption key;
providing the first encryption key for storage in the memory location;
providing the first encryption key to a second encryption engine internal to the monolithic semiconductor device; and
performing an encryption function at the second encryption engine using the first encryption key.

a) Easter fails to disclose or suggest generating a first encryption key based on data from a memory location and providing the first encryption key for storage in the memory location as recited by claim 33

Claim 33 recites the features of: accessing, by a first encryption engine internal to a monolithic semiconductor device, data from a memory location internal to the monolithic semiconductor device, wherein the memory location is accessible only internal to the monolithic semiconductor device; generating, at the first encryption engine, a first encryption key based on the data from the memory location, wherein the data represents a second encryption key; and providing the first encryption key for storage in the memory location. The Office asserts that the key array 25/fuse array 51 of Easter discloses the claimed memory location feature, the RSA engine 57 of Easter discloses the claimed first encryption engine feature, and that Figure 5 of Easter and the passage of Easter at col. 8, lines 18-26 (reproduced above in Section 1) disclose the claimed feature of providing the first encryption key (generated by the first encryption device) for storage in the memory location. Advisory Action, pp. 3-4. The Office elaborates its reasoning by asserting that the passage of Easter at col. 8, lines 18-26 disclose "the public key engine is used to generate the key required by the DES engine and the key is stored in the key array." *Advisory Action*, p. 9. For ease of reference, FIG. 5 of Easter and the cited passage of Easter are reproduced in their entirety:

> Keys for DES encryption engine 21 are stored in key array 25. This is a programmable storage area comprising, for example, RAM. Operationally, keys are transferred for use as DES master keys via public key cryptography techniques using RSA engine 57. One technique for such transfer is described in Munck et al., incorporated by reference hereinabove. Advantageously, using the techniques of the present invention, the private key is secured and the disadvantages of prior manual key loading systems are overcome.

Easter, col. 8, lines 18-26 (emphasis added).



Easter, FIG. 5

Assuming, *arguendo*, that the key array 25/fuse array 51 is equivalent to the claimed memory location feature, the RSA engine 57 is equivalent to the claimed first encryption engine feature, and the DES engine encryption engine 21 is equivalent to the claimed second encryption engine feature as proposed by the Office, Easter would have to disclose or suggest that the RSA engine 57 obtains data from the key array/fuse array 51, generates an encryption key from the data, and stores the generated encryption key in the key array 25/fuse array 51to be consistent with the claimed feature of providing the first encryption key for storage in the memory location

(from which the data used to generate the first encryption key was obtained). However, contrary to the assertions of the Office, Easter fails to disclose or suggest this feature.

As a first issue, even if it is assumed, *arguendo*, that Easter discloses storing an encryption key generated by the RSA engine 57 in the key array 25/fuse array 51, Easter fails to disclose or suggest that data is obtained by the RSA engine 57 from the key array 25/fuse array 51 to generate an encryption key from the obtained data that is then stored in the key array 25/fuse array 51. In other words, Easter fails to disclose or suggest that the RSA engine 57 stores an encryption key in the same memory location that stores the data used by the RSA engine 57 to generate the encryption key. Accordingly, Easter fails to disclose or even suggest the claimed features of generating, at the first encryption engine, a first encryption key based on the data **from the memory location** . . . and providing the first encryption key for storage **in the memory location.**

As a second issue, the cited passage of Easter reproduced above fails to disclose or suggest that any encryption keys generated by the RSA engine 57 are stored in the key array 25/fuse array 51. Rather, this cited passage states "keys are transferred for use as DES master keys via public key cryptography techniques using RSA engine 57. One technique for such transfer is described in Munck, et al. . . . " *Id.* (emphasis added). Thus, this passage merely provides that keys are transferred from the RSA engine 57 for use as DES master keys by the DES engine 21, but this statement by no means expressly provides or even implies that the keys are transferred by storing them in the key array 25/fuse array 51. Rather, turning to FIG. 5 of Easter, Easter illustrates that the connection between the key array 25/fuse array 51 is a unidirectional arrow from the key array 25/fuse array 51 to the RSA engine 57, and Easter does not provide any indication that the connection is bidirectional from the RSA engine 57 to the key

array 25/fuse array 51. FIG. 5 of Easter also fails to illustrate that the output of the RSA engine 57 is connected to an input of the key array 25/fuse array 51 in any manner. In fact, FIG. 5 of Easter fails to illustrate any input to the key array 25/fuse array 51, which is consistent with the written disclosure of Easter. Further, FIG. 5 of Easter illustrates that the only output of the RSA engine 57 is connected to the buses 35 and 35', which input to the DES engine 21. Thus, in view of Figure 5 of Easter and the corresponding disclosure of Easter, one of ordinary skill in the art would appreciate that the RSA engine 57 is connected to the DES engine 21 via the busses 35 and 35' and would not interpret Easter as disclosing or suggesting that an encryption key output by the RSA engine 57 is provided for storage in the key array 25/fuse array 51.

b) The proposed combination of Easter and Van Oorschot fails to disclose or suggest generating a first encryption key based on data from a memory location and providing the first encryption key for storage in the memory location as recited by claim 33

As discussed in section (a) above, Easter fails to disclose or suggest at least the features of generating, at the first encryption engine, a first encryption key based on the data from the memory location and providing the first encryption key for storage in the memory location as recited by claim 33. The Office does not assert that Van Oorschot discloses or suggests these claimed features, nor in fact are these feature disclosed or suggested by Van Oorschot. Accordingly, Easter and Van Oorschot fail to disclose or suggest, individually or in combination, each and every feature recited by claim 33.

c) Claim 33 is allowable under 35 U.S.C. § 103(a)

As discussed in sections (a) and (b) above, the proposed combination of Easter and Van Oorschot fails to disclose or suggest each and every feature recited by claim 33. Accordingly,

the Office fails to establish a *prima facie* case of obviousness in support of its rejection of claim 33. Claim 33 therefore is allowable under 35 U.S.C. § 103(a).

B. Rejection of Claims 17 and 31

In Section 7 of the Advisory Action, claims 17 and 31 were rejected under 35 U.S.C. § 103(a) as unpatentable over Easter in view of Van Oorschot and further in view of Pitts.

1. Rejection of Claim 17

For ease of reference, claim 17 is reproduced in its entirety below:

17. (Previously Presented) A monolithic semiconductor device comprising:
an external data port having an input and an output;
a first encryption engine having an input coupled to the input of said external data port and an output;
a second encryption engine having an input coupled to the output of the first encryption engine and an output;
a memory location having an output coupled to the input of said first encryption engine;
an isolation portion coupled to the output of said memory location and to the input of said external data port, wherein said isolation portion is modifiable to permanently prevent access of said memory location by the external data port; and
wherein the first encryption engine is to provide a first encryption key based on a value stored at said memory location to said second encryption engine.

a) There is no motivation to combine Easter, Van Oorschot and Pitts as proposed by the Office with respect to claim 17

Independent claim 17 recites the features of an external data port having an input and an output, a memory location having an output coupled to an input of a first encryption engine, and an isolation portion coupled to the output of said memory location and to the input of said external data port, wherein said isolation portion is modifiable to permanently prevent access of said memory location by the external data port. The Office acknowledges that Easter and Van Oorschot fail to disclose the claimed isolation portion feature. See Advisory Action, p. 5. The

Office relies on Pitts as disclosing an isolation fuse element that enforces one time programming of the memory. Advisory Action, p. 5. The Office therefore asserts that it would have been obvious "to include a fuse element in the semiconductor device [of Easter] because [a] semiconductor device with [a] fuse is well known in the art. Therefore it would have been obvious . . . to combine the teachings of Pitts within the system of Easter because it prevents external access to the memory location after data has been successfully stored into secure memory array." Id. In contrast with the assertions of the Office, it is respectfully submitted that one of ordinary skill in the art would not be motivated to combine the teachings of Easter and Pitts as proposed.

As noted by the Office, Pitts discloses a technique for preventing *external* access to a memory array 108 via the *external* data path 118 of the circuit 100 by implementing an AND gate 110 and fuse element 112 in the *external* data path 118. *See, e.g., Pitts*, FIG. 1. However, Easter does not disclose that the key array 25/fuse array 51 (which would be analogous to the memory 108 of Pitts) is connected to or accessible an *external* data path of the IC chip 63. Further, Easter provides no indication that the connection of the key array 25/fuse array 51 to an *external* data path of the IC chip 63 would be desirable or advantageous in any way. Thus, as Pitts discloses the use of an AND gate 110 and a fuse 112 at an external data path to prevent *external* access to a memory array, one of ordinary skill in the art would find no motivation to utilize the AND gate 110 and fuse 112 as taught by Pitts in the circuit of Easter as there is no external data path for the key array 25/fuse array 51 in which the AND gate 110 and fuse 112 can be implemented.

Moreover, not only does Easter fail to disclose an external data path for the key array 25/fuse array 51 in which the technique of Pitts can be implemented, Easter teaches that the

external access of the key array 25/fuse array 51 is disadvantageous and is directly contradictory to the stated goal of Easter of "a highly secure single IC chip public key cryptographic system." Easter, col. 2, line 67 – col. 3, line 1; see also Easter, col. 2, lines 63-66 (stating "the use of non-volatile memory for the private key removes security problems associated with loading an IC chip with a value through external means")(emphasis added) and Easter, col. 5, lines 8-11 (stating "the private key for a given system is factory encoded into fuse array 51 of single IC chip 63 before encapsulation. Thus, after the IC chip is encapsulated, only destruction of the IC chip would enable detection of the private key."); see further Easter, col. 8, lines 27-40 (describing the advantages of isolating the fuse array in view of the disadvantages of conventional techniques whereby the private key is loaded from an external source).

Thus, as neither Easter nor Pitts provide any motivation for their combination with the other, and as Easter and Pitts each teaches away from their combination as proposed by the Office, one of ordinary skill in the art would find no motivation to combine the teachings of Easter and Pitts s proposed by the Office. The Office therefore fails to establish a *prima facie* case of obviousness for claim 17.

b) Claim 17 is allowable under 35 U.S.C. § 103(a)

As discussed in section (a) above, there is no motivation to combine the teachings of Easter, Van Oorschot, and Pitts as proposed by the Office to arrive at the particular combination of features recited by claim 17. Accordingly, the Office fails to establish a *prima facie* case of obviousness in support of its rejection of claim 17. Claim 17 therefore is allowable under 35 U.S.C. § 103(a).

2. Rejection of Claim 31

Claims 31 depends from claim 17 and recites the additional feature of at least one silicon die pad coupled to the output of said memory location to provide temporary external access to said memory location.

a) There is no motivation to combine Easter, Van Oorschot and Pitts as proposed by the Office with respect to claim 31

As discussed above with respect to claim 17, one of ordinary skill in the art would find no motivation to combine the teachings of Easter and Pitts s proposed by the Office. The Office therefore fails to establish a *prima facie* case of obviousness for claim 31 at least by virtue of its dependency from claim 17.

b) The proposed combination of Easter, Van Oorschot and Pitts fails to disclose or suggest at least one silicon die pad coupled to the output of a memory location to provide temporary external access to said memory location with respect to claim 31

As discussed above with respect to claims 1 and 41, neither Easter nor Van Oorschot discloses or suggests the claimed features of at least one silicon die pad coupled to the output of a memory location to provide temporary external access to said memory location as recited by claim 31. The Office does not assert that Pitts discloses or suggests this feature, nor in fact is this feature disclosed or suggested by Pitts. The proposed combination of Easter, Van Oorschot and Pitts therefore fails to disclose or suggest at least this claimed feature of claim 31.

c) Claim 17 is allowable under 35 U.S.C. § 103(a)

As discussed in sections (a) and (b) above, not only does the proposed combination of Easter, Van Oorschot and Pitts fail to disclose each and every feature recited by claim 31, there is no motivation to combine the teachings of Easter, Van Oorschot, and Pitts as proposed by the

Office to arrive at the particular combination of features recited by claim 31. Accordingly, the Office fails to establish a *prima facie* case of obviousness in support of its rejection of claims 31. Claim 31 therefore is allowable under 35 U.S.C. § 103(a).

VIII. CONCLUSION

For at least the reasons given above, all pending claims are allowable and the Appellant therefore respectfully request reconsideration and allowance of all claims and that this patent application be passed to issue.

Respectfully submitted,

July 24, 2006
Date

Ryan S. Davidson, Reg. No. 51,596
LARSON NEWMAN ABEL POLANSKY & WHITE, LLP
(512) 439-7100 (phone)
(512) 327-5452 (fax)

IX. APPENDIX OF CLAIMS INVOLVED IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(viii))

The text of each claim involved in the appeal is as follows:

1. (Previously Presented) A monolithic semiconductor device comprising:

a memory location having an output port, wherein a data value to be stored in said memory location is observable only internally to the monolithic semiconductor device;

an asymmetrical encryption engine having an input port coupled to the output port of the memory location and an output port to provide a symmetrical encryption key based on the data value;

a symmetrical encryption engine having an input port coupled to an output port of the asymmetrical encryption engine, wherein the symmetrical encryption engine is to perform an encryption function using the symmetrical encryption key; and

at least one silicon die pad having an input coupled to the output port of said memory location to provide temporary access to said memory location.

17. (Previously Presented) A monolithic semiconductor device comprising:

an external data port having an input and an output;

a first encryption engine having an input coupled to the input of said external data port and an output;

a second encryption engine having an input coupled to the output of the first encryption engine and an output;

a memory location having an output coupled to the input of said first encryption engine;

an isolation portion coupled to the output of said memory location and to the input of said external data port, wherein said isolation portion is modifiable to permanently prevent access of said memory location by the external data port; and

wherein the first encryption engine is to provide a first encryption key based on a value stored at said memory location to said second encryption engine.

31. (Original) The monolithic semiconductor device as in Claim 17, further including at least one silicon die pad coupled to the output of said memory location to provide temporary external access to said memory location.

33. (Previously Presented) A method comprising:

accessing, by a first encryption engine internal to a monolithic semiconductor device, data from a memory location internal to the monolithic semiconductor device, wherein the memory location is accessible only internal to the monolithic semiconductor device;

generating, at the first encryption engine, a first encryption key based on the data from the memory location, wherein the data represents a second encryption key;

providing the first encryption key for storage in the memory location;

providing the first encryption key to a second encryption engine internal to the monolithic semiconductor device; and

performing an encryption function at the second encryption engine using the first encryption key.

41. (Previously Presented) A monolithic semiconductor device comprising:

an encryption engine having an input;

a memory location having an output coupled to the input of the first encryption engine, wherein a data value to be stored in said memory location is observable only internally to the monolithic semiconductor device;

at least one silicon die pad having an input coupled to the output of said memory location to provide temporary access to said memory location.

X. EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

None.

XI. RELATED PROCEEDINGS APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

None.